Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/GB04/005342

International filing date: 21 December 2004 (21.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: GB
Number: 0401627.5
Filing date: 26 January 2004 (26.01.2004)

Date of receipt at the International Bureau: 31 January 2005 (31.01.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PATENT COOPERATION TREATY

From the RECEIVING OFFICE

To:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20
Switzerland

PCT

NOTIFICATION OF DATE OF RECEIPT OF PRIORITY DOCUMENT OR OF PRIORITY APPLICATION NUMBER

(PCT Administrative Instructions, Section 323(a), (b) and (c))

Applicant's or agents's file reference **YWPP17016**	Date of mailing *(day/month/year)* **20/01/2005**
International application No. **PCT/GB2004/005342**	International filing date *(day/month/year)* **21/12/2004 (21 December 2004)**
Applicant **NDS Limited et al**	

1. □ This receiving Office hereby gives notice of the receipt of the priority document(s) identified below on:

2. ☑ This receiving Office hereby gives notice of the receipt of a request (made under Rule 17.1(b)) to prepare and transmit to the International Bureau the priority document(s) identified below on:

21/12/2004 (21 December 2004)

Identification of the priority document(s):

Priority date	Priority application no.	Country or regional Office or PCT receiving Office
26/01/2004 (26 January 2004)	0401627.5	United Kingdom

Name and mailing address of the receiving Office The Patent Office Cardiff Road, Newport South Wales NP10 8QQ Facsimile No.	Authorized officer Neelesh Chillal Telephone No. 01633 814641

PCT/GB 2004/005342

PATENTS • DESIGNS
The Patent Office
COPYRIGHT • TRADE MARKS

CHARTER MARK

INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

I also certify that the attached copy of the request for grant of a Patent (Form 1/77) bears an amendment, effected by this office, following a request by the applicant and agreed to by the Comptroller-General.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 13 January 2005

Patents Form 1/77

Patents Act 1977
(Rule 16)

PATENTS • DESIGNS
The Patent Office
COPYRIGHT • TRADE MARKS

1/77

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
South Wales
NP10 8QQ

1. Your reference

DRW/P17016GB

2. Patent application number
(The Patent Office will fill in this part)

0401627.5

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

NDS LIMITED
One London Road, Staines,
Middlesex, TW18 4EX

07296197002

Patents ADP number *(if you know it)*

If the applicant is a corporate body, give the country/state of its incorporation

4. Title of the invention

TIMELINE PROTECTION

5. Name of your agent *(if you have one)*

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

~~EDWARD EVANS BARKER,~~
~~Clifford's Inn, Fetter Lane,~~
~~London, EC4A 1BZ~~

MARKS & CLERK
90 LONG ACRE
LONDON
WC2E 9RA

G/c.

Patents ADP number *(if you know it)*

240001 ~~05199895001~~ 18001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*
a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

YES

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form

Description 15

Claim *(s)* 5

Abstract

Drawing *(s)* 2 +2

10. If you are also filing any of the following, state how many against each item.

Priority documents

Translations of priority documents

Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*

Request for preliminary examination and search *(Patents Form 9/77)*

Request for substantive examination *(Patents Form 10/77)*

Any other documents *(please specify)*

11. I/We request the grant of a patent on the basis of this application.

Signature

Date 26th January 2004

12. Name and daytime telephone number of person to contact in the United Kingdom Duncan White 02074054916

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) *If you need help to fill in this form or you have any questions, please contact the Patent Office on 08459 500505.*

b) *Write your answers in capital letters using black ink or you may type them.*

c) *If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*

d) *If you have answered 'Yes' Patents Form 7/77 will need to be filed.*

e) *Once you have filled in the form you must remember to sign and date it.*

f) *For details of the fee and ways to pay please contact the Patent Office.*

TIMELINE PROTECTION

FIELD OF THE INVENTION

The present invention relates to audio and video encoding systems, and more particularly to media timelines in video and audio encoding systems and their use by broadcast applications.

BACKGROUND OF THE INVENTION

Published PCT Patent Application WO 02/079955 of NDS Ltd., and corresponding US Patent Application 10/472,286 of Shen Orr et al., the disclosures of which are hereby incorporated herein by reference, describe a system and method for providing variable security mechanisms for securing digital content, in which a single security mechanism is not used for all content. Rather, at least one characteristic or feature of the security mechanism is varied between units, instances or categories of content. Hence, even if unauthorized access is gained to a single unit of content, the overall integrity and security of the system for content distribution is not compromised. Security is preferably provided through a general mechanism, which is then varied in order to provide variable, dissimilar security schemes for different types of content.

The following standards are also believed to be of relevance to the present invention:

ETSI TS 102 822-3 Broadcast and On-line Services: Search, select, and Rightful Use of Content on Personal Storage Systems ("TV-Anytime Phase 1"); Part 3: Metadata.

ISO/IEC 13818-6 Information Technology Generic Coding of Moving Pictures and Associated Audio Information Part 6: Extensions for Digital Storage Media Command and Control.

The disclosures of all references mentioned above and throughout the present specification, as well as the disclosures of all references mentioned in those references, are hereby incorporated herein by reference.

SUMMARY OF THE INVENTION

The term "timeline" is used throughout the present specification and claims to refer to a record of the progression of time from a start of content within a stream of audio / visual data. Metadata and interactive applications can be authored to have specific events occur at specific points of a timeline, thereby synchronizing the metadata and interactive applications to the content. In order to maintain synchronization of metadata or of an interactive application, the timeline for the content needs to pause during advertisement breaks.

However, having a timeline that comprises pauses for advertisement breaks may reveal where advertisement breaks occur in programs. If a Personal Video Recorder (PVR) can determine where an advertisement break is, then the PVR is able to automatically skip the advertisements. Skipping of advertisements puts income to broadcasters from advertisers at risk.

The present invention, in preferred embodiments thereof, provides a method for protecting a timeline so that only authorized devices or applications can access the timeline. The method described can be used to protect platforms without a conditional access system. For example, and without limiting the generality of the foregoing, a terrestrial broadcaster, utilizing the present invention, may securely broadcast, without conditional access protection, a channel that is ordinarily broadcast with conditional access protection by a satellite broadcaster. The terrestrial broadcaster may broadcast the channel without conditional access protection since the timeline associated with content on the channel is encrypted.

The inventor of the present invention believes that there might be moves to reject Normal Play Time (NPT) as the timeline format to use for segmentation information. One possible solution involves timecode delivered in a Packetized Elementary Stream (PES) stream.

The present invention, in preferred embodiments thereof, is based on using a timeline delivered as video timecode; a timecode is a time reference in hours, minutes, seconds, and frames, used to identify a frame. The details of timecode expression are described below, with reference to Appendix A. The timeline can be adapted to work with a system based on defining an offset, for example an offset from the MPEG system time clock (STC) such as normal play time (NPT) (refer to ISO/IEC 13818-6) or an offset from a video timecode.

A timeline delivered as video timecode has a constant stream of timecode (a frame count, for example) closely tied to the video, possibly delivered in the adaptation field of packets or as a separate media stream (such as audio or video) with a Presentation Time Stamp (PTS) for each timecode value. This type of timeline, a preferred implementation of which is described below, is easier to use in a PVR than is NPT.

Timeline values are encrypted using an encryption key. The timeline values can then be decrypted by a trusted device or application.

The use of trusted applications is preferred because using trusted devices is not always possible; for example, and without limiting the generality of the foregoing, use of trusted devices is not generally possible in a horizontal market. Furthermore, the producer of the content and of the application is the party most interested in protecting the timeline, while manufacturers are arguably the ones most interested in opening up the timeline. In preferred embodiments of the present invention, a trusted application can have an embedded decryption key and a decryption algorithm. Moving the location of the key data and changing the algorithm would provide a moving target for receiver manufacturers wishing to implement advertisement skipping.

An implication of the present invention is that the application would manage monitoring the timeline and triggering of stream events. Reducing the frequency of timecode samples and using interpolation to fill in gaps can reduce additional processing overhead. Also, the encryption used does not need to be extremely secure in itself; the security comes more from moving the location of the key data and changing the algorithm. A preferred example of appropriate techniques for moving the location of the key data and changing the algorithm is found in Published PCT Patent Application WO 02/079955 of NDS Ltd., and corresponding US Patent Application 10/472,286 of Shen Orr et al., referred to above and incorporated herein by reference. Also, the inventors of the present invention believe that ad-skipping is not a feature that people or organizations would put endless resources into if encryption were used, because the value of skipping advertisements is low compared to the value of the content itself.

In certain preferred embodiments of the present invention, it is the responsibility of a receiver to pass an encrypted timecode value to the application at the time indicated by the PTS for the timecode value. The receiver cannot determine when a timeline pauses or restarts, or when stream events occur. Therefore the receiver cannot work out where advertisements are from the timeline.

There is thus provided in accordance with a preferred embodiment of the present invention a timecode generation method including receiving an encryption key and an implemented encryption method, for each one of a plurality of frames, receiving a timecode and an associated presentation time stamp (PTS) associated with the one frame, for each one of the plurality of frames, encrypting the timecode associated with the one frame using the encryption key and the implemented encryption method, thereby producing a plurality of encrypted timecodes, and at a time associated with the associated PTS associated with the one frame, outputting a packetized elementary stream (PES) including the plurality of encrypted timecodes.

There is also provided in accordance with another preferred embodiment of the present invention a timecode generation method including receiving an encryption key and an implemented encryption method, for each one of a plurality of frames, receiving a timecode and an associated decoding time stamp (DTS) associated with the one frame, the DTS occurring in advance of a presentation time stamp (PTS) associated with the one frame, for each one of the plurality of frames, encrypting the timecode associated with the one frame using the encryption key and the implemented encryption method, thereby producing a plurality of encrypted timecodes, and at a time associated with the associated DTS associated with the one frame, outputting a packetized elementary stream (PES) including the plurality of encrypted timecodes, the PES including the plurality of encrypted timecodes not being effective until a time associated with the PTS associated with the one frame.

There is also provided in accordance with still another preferred embodiment of the present invention a timecode generator including a first input unit operative to receive an encryption key and an implemented encryption method, a second input unit operative to receive a timecode and an associated presentation time stamp (PTS) for each one of a plurality of frames, an encryptor operative to encrypt the timecode for each one of the plurality of frames, using the encryption key and the implemented encryption method, thereby producing a plurality of encrypted timecodes, and a packetized elementary stream (PES) outputter operative to receive a plurality of encrypted timecodes and, at a time associated with the associated presentation time stamp (PTS) associated with the one frame, to output a PES including the plurality of encrypted timecodes.

There is also provided in accordance with another preferred embodiment of the present invention a timecode use method including receiving an application file including a decryption key and an implemented decryption method, receiving a packetized elementary stream (PES) including a plurality of encrypted timecodes, each of the plurality of timecodes being associated with a presentation time stamp (PTS), and running the application file, the running including:

performing the following when a system time clock (STC) value equals a PTS value associated with at least one of the plurality of encrypted timecodes:

decrypting the encrypted timecode associated with the PTS value using the decryption key and the implemented encryption method, thereby producing a decrypted timecode.

There is also provided in accordance with still another preferred embodiment of the present invention a timecode use method including receiving an application file including a decryption key and an implemented decryption method, receiving a packetized elementary stream (PES) including a plurality of encrypted timecodes, each of the plurality of encrypted timecodes being associated with a decoding time stamp (DTS), at least one of the plurality of encrypted timecodes requiring that a display be updated at one of a plurality of presentation time stamps (PTS), running the application file, the running including:

performing the following when a system time clock (STC) value equals a DTS value associated with at least one of the plurality of encrypted timecodes:

decrypting the encrypted timecode associated with the DTS value using the decryption key and the implemented encryption method, thereby producing a decrypted timecode, and updating the display at the one of the plurality of PTSs.

There is also provided in accordance with another preferred embodiment of the present invention a timecode handler including a first input unit operative to receive at least one application file including a decryption key and an implemented encryption method, a second input unit operative to receive a packetized elementary stream (PES) including a plurality of encrypted timecodes, each of the plurality of encrypted timecodes being associated with a presentation time stamp (PTS), and a decryptor receiving each of the plurality of encrypted timecodes and operative to decrypt each of the plurality of encrypted timecodes using the decryption key and the implemented encryption method when a system time clock (STC) value equals a PTS value associated with each of the plurality of encrypted timecodes.

There is also provided in accordance with still another preferred embodiment of the present invention a method for timeline protection including receiving, at a timecode generator, an encryption key and an implemented encryption method, for each one of a plurality of frames, receiving, at the timecode generator, a timecode and an associated presentation time stamp (PTS) associated with the one frame, for each one of the plurality of frames, encrypting, at the timecode generator, the timecode associated with the one frame using the encryption key and the implemented encryption method, thereby producing a plurality of encrypted timecodes, at a time associated with the associated presentation time stamp (PTS) associated with the one frame, outputting a packetized elementary stream (PES) including the plurality of encrypted timecodes, receiving, at a timecode handler, an application file including a decryption key and an implemented decryption method, receiving, at the timecode handler, the PES including a plurality of encrypted timecodes, each of the plurality of timecodes being associated with a presentation time stamp (PTS), and running the application file, the running including:

at the application file, performing the following when a system time clock (STC) value equals a PTS value associated with at least one of the plurality of encrypted timecodes:

decrypting the encrypted timecode associated with the PTS value using the decryption key and the implemented encryption method, thereby producing a decrypted timecode.

There is also provided in accordance with another preferred embodiment of the present invention a system for timeline protection including a timecode generator including:

a timecode generator first input unit operative to receive an encryption key and an implemented encryption method, a timecode generator second input unit operative to receive a timecode and an associated presentation time stamp (PTS) for each one of a plurality of frames, a timecode generator encryptor operative to encrypt the timecode for each one of the plurality of frames, using the encryption key and the implemented encryption method, thereby producing a plurality of encrypted timecodes, a timecode generator packetized elementary stream (PES) outputter operative to receive a plurality of encrypted timecodes and, at a time associated with the associated presentation time stamp (PTS) associated with the one frame, to output a PES including the plurality of encrypted timecodes, and a timecode handler including:

a timecode handler first input unit operative to receive at least one application file including a decryption key and an implemented decryption method, a timecode handler second input unit active to receive the PES including a plurality of encrypted timecodes, each of the plurality of encrypted timecodes being associated with a presentation time stamp (PTS), and a timecode handler decryptor receiving each of the plurality of encrypted timecodes and operative to decrypt each of the plurality of encrypted timecodes using the decryption key and the implemented encryption method when a system time clock (STC) value equals a PTS value associated with each of the plurality of encrypted timecodes.

BRIEF DESCRIPTION OF THE DRAWINGS AND APPENDICES

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

Fig. 1 is a simplified partly pictorial partly block diagram illustration of a system for timecode protection, constructed and operative in accordance with a preferred embodiment of the present invention; and

Fig. 2 is a graphical diagram of timeline plotted against System Time Clock (STC), useful for understanding the system of Fig. 1.

The following Appendices may be helpful in understanding certain preferred embodiments of the present invention:

Appendix A is a tabular presentation of the format of a preferred embodiment of a timecode packet for unencrypted timecode values, and of an encryption header for delivering the timecode packet; and

Appendix B is a discussion of multiple timelines in the context of the system of Fig. 1.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

Reference is now made to Fig. 1, which is a simplified partly pictorial partly block diagram illustration of a system for timecode protection, constructed and operative in accordance with a preferred embodiment of the present invention. In the description of Fig. 1, a preferred embodiment of the present invention is described as implemented in a broadcast headend and a broadcast receiver. The implementation described can be adapted in a number of ways. For example, and without limiting the generality of the foregoing, the present invention may be adapted for audio-only content or by using different methods of encryption (such as, for example, public/private encryption, symmetric encryption, or any other appropriate type of encryption).

A possible enhancement of a preferred implementation of the present invention is to use both decode time stamps (DTS) and presentation time stamps (PTS) for PES carrying timecode values. The application is passed an encrypted timecode value when STC=DTS, giving the application time to prepare for a display to be updated when the PTS occurs.

It is appreciated that the headend and the receiver preferably comprise conventional elements implemented in hardware and software. For ease of depiction, as well as in the interest of brevity, only portions of the headend or receiver relevant to the present invention are depicted or described. For example, and without limiting the generality of the foregoing, conventional components used for audio encoding, A/V encryption, and so forth, are all omitted from the figures and description.

The following discussion describes various components comprised in the headend and receiver, and which are utilized in preferred embodiments of the present invention:

I. Headend

A. Application Playout

An interactive application using an encrypted timeline is preferably provided as two parts: the data files to be broadcast; and the encryption key and algorithm to use at the headend. The application playout preferably provides the application data to a carousel generator and to a timecode generator just prior to broadcast of content to which the interactive application is synchronized.

Application code comprises a timecode-decrypting algorithm and at least one of a plurality of application files comprises a timecode-decrypting key. These parts of the interactive application are preferably obfuscated. For example, and without limiting the generality of the foregoing, the method and system described in Published PCT Patent Application WO 02/079955 of NDS Ltd., and corresponding US Patent Application 10/472,286 of Shen Orr et al., referred to above and incorporated herein by reference, would provide an appropriate method and system for obfuscating the parts of the interactive application.

B. Carousel Generator

The carousel generator delivers the plurality of application files in a delivery format such as the Digital Storage Media - Command and Control (DSM-CC) object carousel or data carousel.

C. Timecode Generator

The encryption key and details on an encryption algorithm are preferably provided to the timecode generator. The timecode generator also receives a feed of timing information from a video encoder, which provides the values of the timecode plus the PTS of a corresponding video frame.

The timecode generator preferably uses the encryption algorithm expected by the interactive application. Downloading a new application, which implements a different encryption algorithm, easily changes the encryption algorithm, thereby making it disadvantageous to implement receivers that can crack one specific algorithm. It is appreciated that the application is preferably broadcast by a carousel, as is well known in the art, so the application is frequently available for download.

The timecode generator creates a PES stream comprising values of timecode encrypted using the encryption algorithm and encryption key specified by the interactive application. The PES stream comprising the timecode is synchronized to a video using the PES packet structure to associate one of a plurality of PTSs with each encrypted timecode value. A specific PTS associated with an encrypted timecode value matches that of the corresponding encoded video frame from the video encoder.

It may not be necessary to insert a timecode value for every frame. For example, and without limiting the generality of the foregoing, a PVR may use the present invention if only the encrypted timecode values for the first frames of Groups of Pictures (GOPs) is inserted.

The timecode generator preferably produces timecode irrespective of whether an application requires the values; otherwise, the absence of information may be sufficient to indicate where advertisements are, thereby enabling ad-skipping by PVRs and other similar devices.

D. Video Encoder

In addition to encoding video, the video encoder provides timecode-to-PTS information to the timecode generator. Many MPEG video encoders embed Vertical Interval Timecode (VITC) timecode in GOP headers, thereby providing timecode-to-PTS information. The timecode generator can then extract the timecode-to-PTS information from the encoded video.

E. Multiplexer

The multiplexer is preferably configured using standard methods known in the art to accept the new timecode elementary stream.

II. Receiver

A. Demultiplexer

The demultiplexer is preferably configured by software comprised in the receiver to extract the PES associated with a service as a whole from the transport stream.

The demultiplexer preferably feeds the interactive application data (comprising the decryption key) to a carousel client. The demultiplexer passes the timecode elementary stream, comprising the encrypted values of timecode, to the timecode handler. The demultiplexer passes the encoded video to the video decoder.

It is appreciated that many different configurations of receiver hardware and software may be used in order to implement the demultiplexer functionality.

B. Carousel Client

The carousel client preferably retrieves interactive application code for execution by the receiver. Once running, the interactive application preferably uses the carousel client to retrieve files from a broadcast carousel. The decryption key is embedded in retrieved files so as to hide them from software resident in the receiver.

C. Timecode Handler

The timecode handler is a receiver module that passes the encrypted timecode values to the interactive application when a system time clock (STC) value equals the time given by the PTS for the timecode PES packet.

D. Video Decoder

The video decoder outputs decoded video and provides STC information to the timecode handler.

E. Running Interactive Application

Executing the application code delivered by the broadcast carousel preferably produces a running interactive application. The running interactive application comprises the algorithm for decoding the encrypted timecode values. The key for decrypting these values is provided in resource files for the application.

The application resource files detail which values of the timecode comprise one of a plurality of synchronization points occurring in the video. The running interactive application preferably decrypts and monitors incoming timecode values. When one of the plurality of synchronization points occurs, the running interactive application preferably then updates a video display or the application's behavior in a way that is synchronous with the video.

If there are "gaps" in the incoming timecode, the application interpolates the intermediate values. For example, and without limiting the generality of the foregoing, a timecode value may only be given for the first frame of a GOP. To perform such an interpolation requires additional triggers, which indicate to the application when intermediate frames are displayed, for the in-between frames. Either the timecode handler or the video decoder preferably provides these triggers.

Reference is now made to Appendix A, which is a tabular presentation of the format of a preferred embodiment of a timecode packet for unencrypted timecode values, and of an encryption header for delivering the timecode packet. A basic textual syntax for timecode is HH:MM:SS:FF, where HH is hours, MM is minutes, SS is seconds, and FF is frames.

The format of the timecode packet for unencrypted timecode information is given in Table 1 of Appendix A. The timecode_id field uniquely identifies a particular timeline, allowing for multiple consecutive timelines. The status field indicates if the particular timeline is running or paused.

The timecode packet structure is preferably encrypted using any appropriate type of encryption, as described above, into a sequence of encrypted bytes and placed in an encryption container, given in Table 2 of Appendix A. The encryption container is then inserted into a PES packet.

Reference is now made to Appendix B, which is a discussion of multiple timelines in the context of the system of Fig. 1. In a broadcast environment it is necessary to distinguish between multiple timelines. For example, one timeline may be for an interactive advertisement and another timeline may be for the current program.

It is appreciated that various features of the invention which are, for clarity, described in the contexts of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable subcombination.

It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the invention is defined only by the claims which follow:

APPENDIX A

Table 1: Unencrypted timecode values

Syntax	Bits	Mnemonic
timecode_packet() {		
num_values	8	uimsbf
for (i=0; i<num_values; i++) {		
timecode_id	8	
hours	5	uimsbf
minutes	6	uimsbf
seconds	6	uimsbf
frames	5	uimsbf
status	2	bslsbf
}		
}		

Table 2: Encryption container

Syntax	Bits	Mnemonic
encryption_container() {		
encryption_type	16	uimsbf
num_encrypted_bytes	8	uimsbf

for (i=0; i<num_encrypted_bytes; i++)
{		

encrypted_timecode_byte	8	bslsbf
}		
}		

APPENDIX B

Reference is now made to Fig. 2, which is a graphical diagram of timeline plotted against System Time Clock (STC), useful for understanding the system of Fig. 1.

The receiver preferably uses the timecode reference data conveyed in a timeline to compute Universal Co-ordinated Time (UTC) and STC values for a given content item, designated as content_id, and timeline pair. The reference data conveys entries for each discontinuity in STC with respect to timeline.

Consider the following example where a single SI-event experiences the following transitions:

1. the event starts with its main program content (content_id=0) at STC=A
2. the event moves to commercial break and switches to content_id=1 at STC=B
3. the event switches back to the main program content at STB=C
4. an STC discontinuity occurs at STC=D where the STC is set to E. (Note, in the diagram E > D, but this may not be so in reality)

CLAIMS

1. A timecode generation method comprising:

receiving an encryption key and an implemented encryption method;

for each one of a plurality of frames, receiving a timecode and an associated presentation time stamp (PTS) associated with the one frame;

for each one of the plurality of frames, encrypting the timecode associated with the one frame using the encryption key and the implemented encryption method, thereby producing a plurality of encrypted timecodes; and

at a time associated with the associated PTS associated with the one frame, outputting a packetized elementary stream (PES) comprising the plurality of encrypted timecodes.

2. A timecode generation method comprising:

receiving an encryption key and an implemented encryption method;

for each one of a plurality of frames, receiving a timecode and an associated decoding time stamp (DTS) associated with the one frame, the DTS occurring in advance of a presentation time stamp (PTS) associated with the one frame;

for each one of the plurality of frames, encrypting the timecode associated with the one frame using the encryption key and the implemented encryption method, thereby producing a plurality of encrypted timecodes; and

at a time associated with the associated DTS associated with the one frame, outputting a packetized elementary stream (PES) comprising the plurality of encrypted timecodes, the PES comprising the plurality of encrypted timecodes not being effective until a time associated with the PTS associated with the one frame.

3. A timecode generator comprising:

a first input unit operative to receive an encryption key and an implemented encryption method;

a second input unit operative to receive a timecode and an associated presentation time stamp (PTS) for each one of a plurality of frames;

an encryptor operative to encrypt the timecode for each one of the plurality of frames, using the encryption key and the implemented encryption method, thereby producing a plurality of encrypted timecodes; and

a packetized elementary stream (PES) outputter operative to receive a plurality of encrypted timecodes and, at a time associated with the associated presentation time stamp (PTS) associated with the one frame, to output a PES comprising the plurality of encrypted timecodes.

4. A timecode use method comprising:

receiving an application file comprising a decryption key and an implemented decryption method;

receiving a packetized elementary stream (PES) comprising a plurality of encrypted timecodes, each of the plurality of timecodes being associated with a presentation time stamp (PTS); and

running the application file, the running comprising:

performing the following when a system time clock (STC) value equals a PTS value associated with at least one of the plurality of encrypted timecodes:

decrypting the encrypted timecode associated with the PTS value using the decryption key and the implemented encryption method, thereby producing a decrypted timecode.

5. A timecode use method comprising:

receiving an application file comprising a decryption key and an implemented decryption method;

receiving a packetized elementary stream (PES) comprising a plurality of encrypted timecodes, each of the plurality of encrypted timecodes being associated with a decoding time stamp (DTS), at least one of the plurality of encrypted timecodes requiring that a display be updated at one of a plurality of presentation time stamps (PTS);

running the application file, the running comprising:

performing the following when a system time clock (STC) value equals a DTS value associated with at least one of the plurality of encrypted timecodes:

decrypting the encrypted timecode associated with the DTS value using the decryption key and the implemented encryption method, thereby producing a decrypted timecode; and

updating the display at the one of the plurality of PTSs.

6. A timecode handler comprising:

a first input unit operative to receive at least one application file comprising a decryption key and an implemented encryption method;

a second input unit operative to receive a packetized elementary stream (PES) comprising a plurality of encrypted timecodes, each of the plurality of encrypted timecodes being associated with a presentation time stamp (PTS); and

a decryptor receiving each of the plurality of encrypted timecodes and operative to decrypt each of the plurality of encrypted timecodes using the decryption key and the implemented encryption method when a system time clock (STC) value equals a PTS value associated with each of the plurality of encrypted timecodes.

7. A method for timeline protection comprising:

receiving, at a timecode generator, an encryption key and an implemented encryption method;

for each one of a plurality of frames, receiving, at the timecode generator, a timecode and an associated presentation time stamp (PTS) associated with the one frame;

for each one of the plurality of frames, encrypting, at the timecode generator, the timecode associated with the one frame using the encryption key and the implemented encryption method, thereby producing a plurality of encrypted timecodes;

at a time associated with the associated presentation time stamp (PTS) associated with the one frame, outputting a packetized elementary stream (PES) comprising the plurality of encrypted timecodes;

receiving, at a timecode handler, an application file comprising a decryption key and an implemented decryption method;

receiving, at the timecode handler, the PES comprising a plurality of encrypted timecodes, each of the plurality of timecodes being associated with a presentation time stamp (PTS); and

running the application file, the running comprising:

at the application file, performing the following when a system time clock (STC) value equals a PTS value associated with at least one of the plurality of encrypted timecodes:

decrypting the encrypted timecode associated with the PTS value using the decryption key and the implemented encryption method, thereby producing a decrypted timecode.

8. A system for timeline protection comprising:

a timecode generator comprising:

a timecode generator first input unit operative to receive an encryption key and an implemented encryption method;

a timecode generator second input unit operative to receive a timecode and an associated presentation time stamp (PTS) for each one of a plurality of frames;

a timecode generator encryptor operative to encrypt the timecode for each one of the plurality of frames, using the encryption key and the implemented encryption method, thereby producing a plurality of encrypted timecodes;

a timecode generator packetized elementary stream (PES) outputter operative to receive a plurality of encrypted timecodes and, at a time associated with the associated presentation time stamp (PTS) associated with the one frame, to output a PES comprising the plurality of encrypted timecodes; and

a timecode handler comprising:

a timecode handler first input unit operative to receive at least one application file comprising a decryption key and an implemented decryption method;

a timecode handler second input unit active to receive the PES comprising a plurality of encrypted timecodes, each of the plurality of encrypted timecodes being associated with a presentation time stamp (PTS); and

a timecode handler decryptor receiving each of the plurality of encrypted timecodes and operative to decrypt each of the plurality of encrypted timecodes using the decryption key and the implemented encryption method when a system time clock (STC) value equals a PTS value associated with each of the plurality of encrypted timecodes.

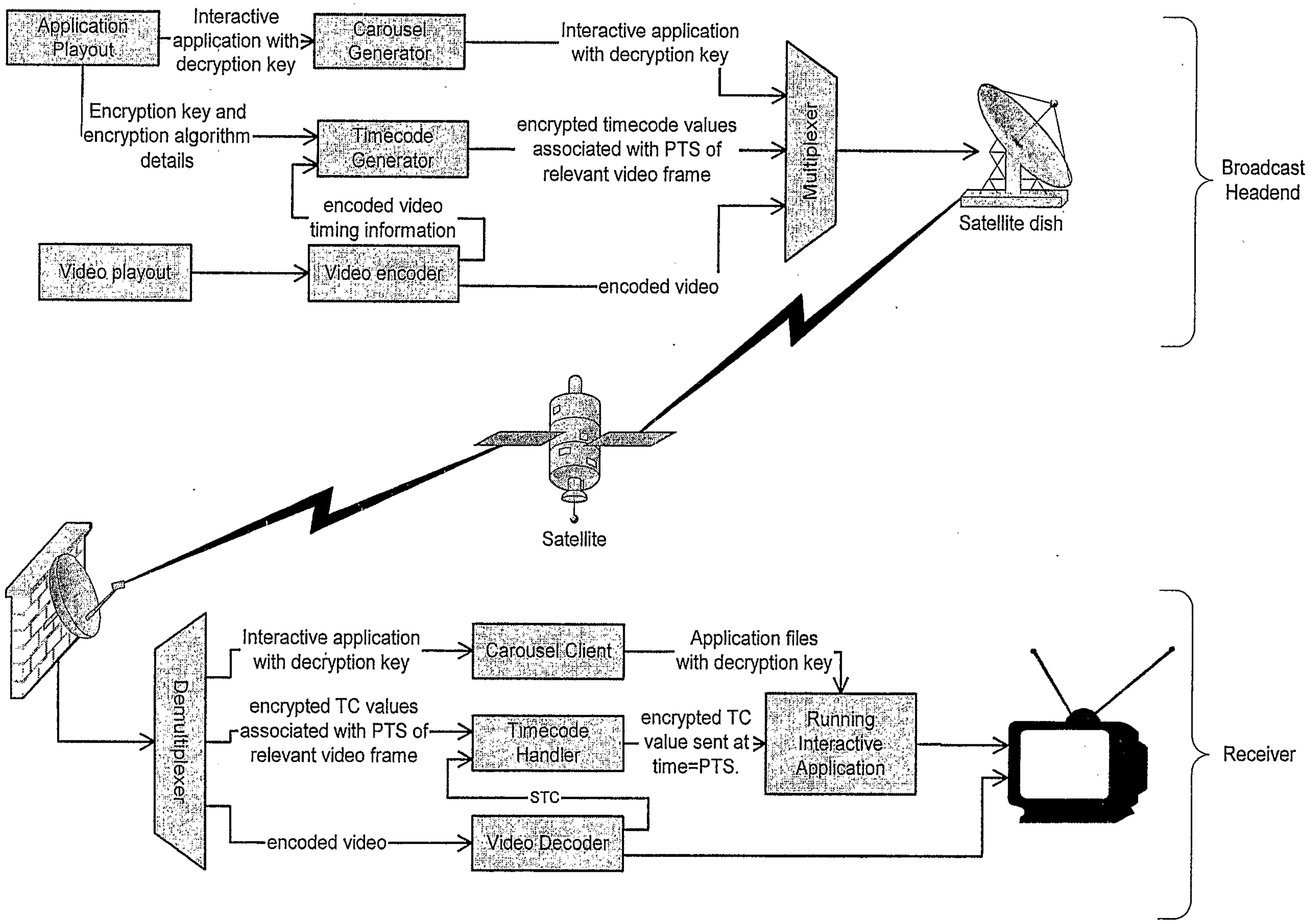
Application Playout
Interactive application with decryption key
Carousel Generator
Interactive application with decryption key
Encryption key and encryption algorithm details
Timecode Generator
encrypted timecode values associated with PTS of relevant video frame
encoded video timing information
Video playout
Video encoder
encoded video
Multiplexer
Satellite dish
Broadcast Headend
Satellite
Demultiplexer
Interactive application with decryption key
Carousel Client
Application files with decryption key
encrypted TC values associated with PTS of relevant video frame
Timecode Handler
encrypted TC value sent at time=PTS.
Running Interactive Application
STC
encoded video
Video Decoder
Receiver

Figure 1

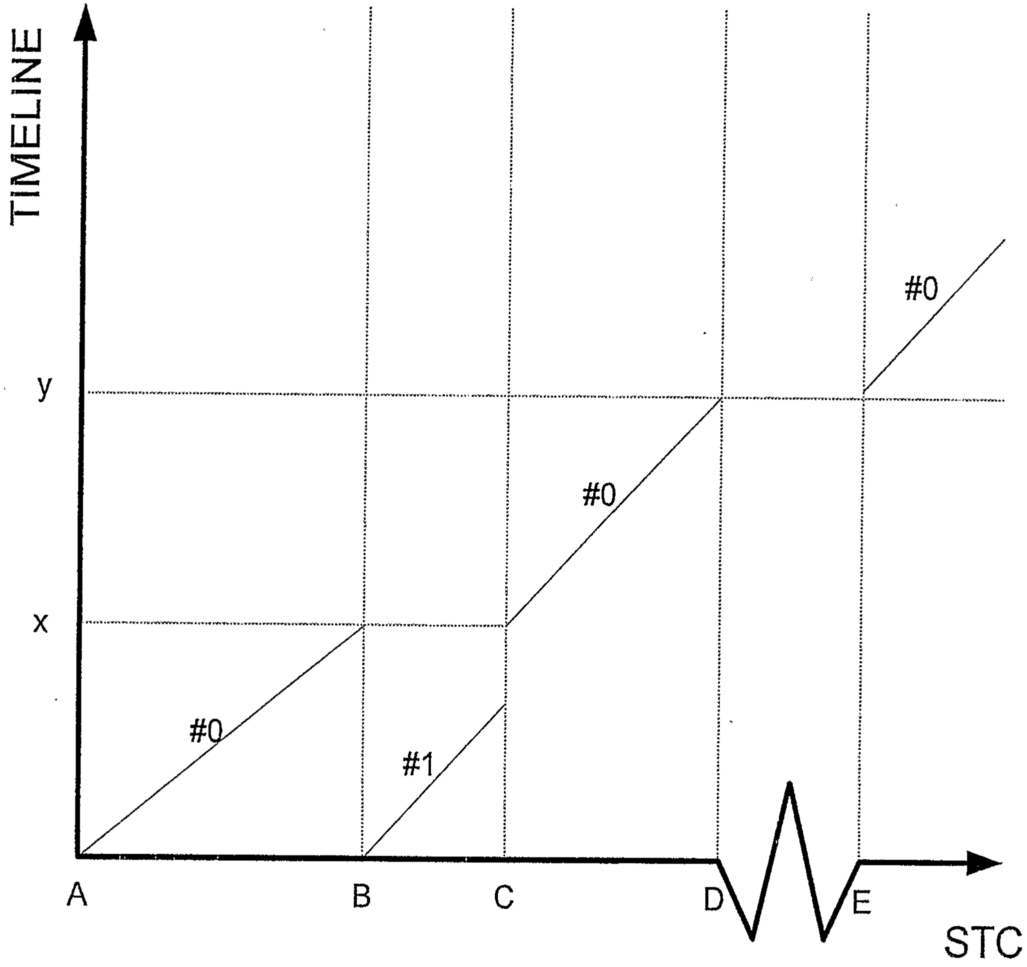

Figure 2

PCT/GB2004/005342

21/12/04

MARKS & CLERK.